CERTICOM FAQ SERIES

FAQ : Certicom ZigBee Smart Energy

CERTIFICATE SERVICE AND ZIGBEE SMART ENERGY SDK LICENSING

February 2011

certicom™

CONTENTS

1. What are ZigBee Smart Energy device certificates?

A device certificate is a digital ID which binds device information such as a device MAC address and manufacturing information to a public key pair using a signature from a trusted third party Certification Authority.

Each device should contain its own unique device certificate. The certificate is used to uniquely authenticate a device on the network using its private and public key pair. These keys allows the device to authenticate itself on a network, perform efficient and secure authenticated key agreement and perform digital signature operations.

ZigBee Smart Energy (ZSE) 1.0 device certificates are Elliptic Curve Qu Vanstone (ECQV) implicit certificates which bind MAC addresses and ZigBee Smart Energy Profile (0109 h) attribute data to an ECC key pair. See http://en.wikipedia.org/wiki/Implicit_certificate for an explanation of the underlying cryptography.

The Certicom Device CA for ZigBee Smart Energy provides a common root of trust for ZigBee Smart Energy Profile test or production devices, enabling out of the box interoperability and security, lowering the total cost of ownership for utilities and metering companies while enhancing the security and integrity of the utility network devices with a bandwidth efficient public key infrastructure (PKI).

The Certicom ZigBee Smart Energy PKI service issues Elliptic Curve Qu Vanstone (ECQV) implicit certificates to eligible, licensed subscribers – production certificates to ZigBee Alliance members with ZigBee Smart Energy Profile Certified devices and test certificates to developers building and testing new Smart Energy products.

ECQV certificates are used to secure a ZigBee Smart Energy device as it gets enrolled on the network using an authenticated key agreement scheme, and further to sign a device's Smart Energy Profile messages.

2. What are test certificate and production certificates?

A test certificate is a low-assurance ZigBee device certificate issued through Certicom's website. Test certificates works identically to production certificates but they should not be relied upon for any purpose other than testing.

To enhance network security, the Test CA and Production CA elliptic curve key pairs are different, as are the assurance levels. Test and production certificates are not meant to interoperate.

The test CA's ID is: 5445535453454341
The **Test CA public key** (in compressed format) is:
0200fde8a7f3d1084224962a4e7c54e69ac3f04da6b8

The production CA's ID is: 0022080000000001
The **Production CA public key** (in compressed format) is:
0202264c5e4cbfa186a6b925b966b5b3a4d7a390344e

Note that you don't actually need to program the device's public key into the device. The other device calculates the public key based on the cert it receives. That's one of the things that the CA public key is used for, as described in the Wikipedia reference on computing the public key from the implicit certificate.

Certicom's ZigBee PKI protects the production certificate private key in a high security environment. The service follows strict issuance procedures which validate the identity and eligibility of subscriber companies, logging all certificates issued on behalf of a manufacturer.

Certicom's test certificate license and SDK license prohibit the use of test certificates in a production environment. Test certificates are only authorized for use only development and test environments.

Only ZigBee Smart Energy Certified devices are licensed to use production certificates. Pilot deployments must use certified devices and production certificates, not devices with test certificates. À la carte pricing allows smaller companies

3. What is Profile Attribute Data?

For ZigBee Smart Energy 1.0 Profile Attribute data is 10 bytes of data you supply to Certicom's CA for device certificate issuance. This information is bound to the device certificate along with the device MAC address by the issuing CA private key. The corresponding CA public key is used to compute the device public key.

For test certificates, Profile Attribute data can be anything you like. This supports positive and negative compliance testing.

While the Certicom PKI does not check what MAC address or Profile Attribute data is used for test certificates, production certificate requests must provide unique MAC addresses for each device and a valid Profile Attributed data request.

While the profile attribute data fields are set by the requestor, some of the fields on production certificates are overwritten by the CA (e.g. Certificate Version) on certificate issuance, other fields are simply checked for validity, e.g. that the MFG ID matches the company requesting the certificate.

For production certificates the MFG ID should match the one your company has been issued by the ZigBee Alliance. The values we expect are hex characters, ab:cd used as an example. For test certificates this up to the user and no validation is done by the CA.

```
Profile Attribute Data (10 bytes) =
{
Profile ID (2 bytes=01:09) – set by requestor, validated by production CA vetting service
+cert version (2 bytes =00:00) – set by requestor, overwritten by production CA)
+manufacture ID(2 bytes = ab:cd) – set by requestor as their MFG ID, validated by
production CA vetting service
+customer data(4 bytes = xx:xx:xx:xx) – set by requestor, ignored by CA
}
```

You can optionally also specify 4 bytes of MFG data for your device model number, etc. Here 00:00:00:01 is used as an example.

E.g., a request with Profile Attribute Data = 01090000106300000001 {request with Profile ID 01:09, MFG ID 10:63, MFG optional data 00:00:00:01 }

As issued: Profile Attribute Data = 01091083106300000001 {after the Certicom production CA has issued the certificate, setting CA version and other flags }

What a specific ZigBee stack does when they parse the certificate within the device is implementation specific but stacks should check the Profile ID to verify a Smart Energy Profile device (0109 hex).

4. Who is eligible to purchase production certificates?

Certificates are licensed to ZigBee Alliance OEMs for use in their own *Certified* ZigBee Alliance Smart Energy Profile products. Certificates are licensed to each company separately and usage must be carefully controlled and tracked.

Multiple devices cannot use the same certificate – each device must have its own. Likewise OEMs may not share their certificates with other companies or use them in non-certified products. These restrictions help reinforce the trust model requirements and interoperability goals of a successful standard.

5. What are the licensing options for production certificates?

Certificates are available through a subscription or à la carte license. À la carte pricing allows companies entering the market access to Certicom technology at a lower upfront cost. Subscription licenses offer lower per unit prices in exchange for an annual commitment.

6. What are the licensing options for production certificates?

Certificate pricing is provided in Certicom's license agreements. For your convenience a schedule is provided in the table below.

Certicom ZigBee Smart Energy (ZSE) Certificate Pricing

À la Carte License Pricing

Minimum Quantity Per Order	Annual Fee	Per-Order Fee	Per-Device Fee	Minimum Order Cost
500	$0	$1000	$1.00	$1,500.00
5000	$0	$1000	$.40	$3,000.00
20,000	$0	$1000	$.32	$7,400.00
50,000	$0	$1000	$.26	$14,000.00
100,000	$0	$1000	$.21	$22,000.00

Annual Subscription License Pricing – 1 Year Term

Minimum Quantity Per Order	Annual Fee	Per-Order Fee	Per-Device Fee
1	$15,000	$1000	$0.07
>=250,000	$15,000	$0	$0.07

7. Can I get a device certificate from an entity besides Certicom?

At present Certicom is the only entity authorized to issue ZigBee Smart Energy 1.0 certificates. A single Certificate Authority (CA) allows any ZigBee Certified device to authenticate with any other ZigBee Certified device, regardless of where in the world these devices are manufactured.

8. Do I need to pay for test certificates?

No, test certificates are freely available to companies and individuals who register their details with Certicom at www.certicom.com/index.php/gencertregister. Validation is required to ensure the service is not abused. More information is available at: www.certicom.com/index.php/device-authentication-service/smart-energy-device-certificate-service

9. Will certificate pricing change in the future?

Certicom ZigBee Smart Energy 1.0 certificate fees are subject to change but increases are capped in the subscriber license agreements.

10. What are Certicom Smart Energy security libraries?

Certicom provides ZigBee Smart Energy (ZSE) libraries which implement the Certificate Based Key Establishment (CBKE) protocol and ECC-based digital signature operations to stimulate the development of ZigBee products. ZigBee members benefit by getting their products to market quickly using a secure, optimized ZSE implementation from domain experts, providing additional assurances of correctness and support.

11. How much do Certicom ZSE libraries cost?

Certicom ZigBee Smart Energy 1.0 libraries are now free for both development and distribution. Free libraries do not include support. Licenses can be obtained by applying at:

www.certicom.com/index.php?option=com_chronocontact&chronoformname=certicom_zigbee_sdk_registration_form

From time to time new versions may be made available to support new silicon platforms or compiler tool chains. Porting may be offered for additional fees but all resulting product, patents and trade secret optimizations remain the property of Certicom. Contact ZigBeeSales@Certicom.com for information.

12. Must I use Certicom ZSE libraries?

No. Companies are free to implement their own ZSE library but must still use Certicomlicensed certificates.

13. Why should I consider Certicom ZSE runtime libraries?

Certicom SDKs provide fast time-to-market through pre-integration with third-party ZigBee stacks, size and performance optimizations for resource-constrained system-on-chip designs.

14. What are some of the benefits of working with Certicom?

Certicom products deliver considerable value to ZigBee members wishing to implement the ZigBee Smart Energy profile or any other security scheme requiring expertise in public key technology and key management.

First and foremost, Certicom is committed to ongoing expertise in cryptology specializing in Elliptic Curve Cryptography (ECC). It is important to note that cryptology is a dynamic field that pits cryptanalyst against cryptographers. As such Certicom employs cryptologists who are experts in both cryptanalysis and cryptography, and keeps them focused on elliptic curve cryptology. We are embedded in the cryptology community and are usually first to be made aware of any general cryptanalytical advancement as well as specific ones that might pertain to implementations used in ZigBee. As such, we are poised to react quickly when new techniques or vulnerabilities are discovered.

Intellectual property is not merely patents, but broadly encompasses Certicom research and development expertise building and fielding cryptographic systems. Trade secret know-how has been developed through many years, allowing us to create optimizations and space/performance trade-offs on a per-processor basis.

About Certicom

Certicom, a wholly owned subsidiary of Research In Motion Limited (RIM) (Nasdaq: RIMM; TSX: RIM), manages and protects the value of content, applications and devices with government-approved security. Adopted by the National Security Agency (NSA) for government communications, Elliptic Curve Cryptography (ECC) provides the most security per bit of any known public-key scheme. As the global leader in ECC, Certicom's security offerings are currently licensed to hundreds of multinational technology companies, including IBM, General Dynamics, Motorola and Oracle. Founded in 1985, Certicom's corporate office is located in Mississauga, Ontario, Canada with worldwide sales offices in USA and Asia. Visit www.certicom.com.

Corporate Headquarters
5520 Explorer Drive, 4th Floor
Mississauga, ON L4W 5L1
Canada
Tel: 1.905.507.4220
Toll Free: 1.800.561.6100
(NA only)
info@certicom.com

USA
3600 Glen Canyon Rd., Suite 1
Scotts Valley, CA 95066
USA
Tel: 1.831.438.4100
Fax: 1.831.438.4111
Sales: 1.800.561.6100
sales@certicom.com

Japan
Research In Motion Japan Ltd.
Nippon Brunswick, Building 7F
5-27-7 Sendagaya,Shibuya-ku,
Tokyo 151-0051, Japan
Tel: 03 6367 3567
sales@certicom.com

*A Subsidiary
of Research In Motion Limited*

certicom™

Additional Certicom White Papers

To read other Certicom white papers, please visit www.certicom.com.

Sum Total: Determining the True Cost of Security
Sourcing Security: Five Arguments in Favour of Commercial Security Solutions

Government

Making the Grade: Meeting Government Security Requirements (Suite B)
Meeting Government Security Requirements: The Difference Between Selling to the Government and Not
FAQ: The National Security Agency's ECC License Agreement with Certicom Corp.

Mobility

The Inside Story
Many Happy Returns: The ROI of Embedded Security
Welcome to the Real World: Embedded Security in Action

Sensor Networks

Securing Sensor Networks

DRM & Conditional Access

Injecting Trust to Protect Revenue and Reputation: A Key Injection System for Anti-Cloning, Conditional Access and DRM Schemes
Achieving DRM Robustness: Securing the Device from the Silicon Up to the Application(PDF)

Enterprise Software

Using Digital Signatures to cut down on Bank Fraud Loss

ECC

An Elliptic Curve Cryptography Primer
ECC in Action: Real World Applications of Elliptic Curve Cryptography
Using ECC for Enhanced Embedded Security (PDF)